USER GUIDE

T2-2500 PowerBroadband
(aka mT2a EthernetXD)

Motorola, Inc. 549453-001-00-a

No part of this publication may be reproduced or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the publisher.
Information in this manual is furnished under license and may only be used in accordance with the terms of the software license. This publication and the information herein is furnished AS IS, is subject to change without notice, and should not be construed as a commitment by Motorola. Motorola assumes no responsibility or liability for any errors or inaccuracies, makes no warranty of any kind (expressed, implied, or staory) with respect to this publication, and expressly disclaims any and all warranties of merchantability, fitness for particular purposes, and noninfringement of third-party rights.
Companies, names, and data used in the examples herein are fictitious unless otherwise noted.

Pass-Through Licenses:

Net-SNMP	Copyright 1989, 1991, 1992, 1996, 1998-2004
LwIP	Copyright © 2001, 2002 Swedish Instie of Computer Science

Net-SNMP and LwIP source code are provided under the terms of their respective license agreements.

Source code and copyright notices are available from Motorola support.
email: pbn.support@motorola.com

Copyright © 2005-2006 Motorola, Inc. All rights reserved.
'Motorola' is a registered trademark of Motorola, Inc. in the United States and in other countries.
Other trade names used in this document are trademarks or registered trademarks of the manufacturers or vendors of the associated products.

Motorola, Inc.
5200 Franklin drive, Suite 100
Pleasanton, CA 94588
1 (925) 201-4500 main
1 (925) 201-4509 fax
1 (800) 998-4888
www.systems.com
Published in the United States of America
August, 2007
T2-2500 PowerBroadband User Guide
Text part number: 549453-001-00 rev A

Model Number: 45125
45101

Radio Frequency Interference Requirements- FCC

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Radio Frequency Interference Requirements- Canada

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Marking and European Economic Area (EEA)

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Statement of Compliance

Motorola/Symbol hereby declares that this device is in compliance with all the applicable Directives, 2004/108/EC and 2006/95/EC. A Declaration of Conformity may be obtained from http://www2.symbol.com/doc/.

IMPORTANT SAFETY INSTRUCTIONS

mT2a Switch
CAUTION: For installation only in a Restricted Access Location by trained service personnel.
CAUTION: Equipment must be connected to an earthed mains socket-outlet.
CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
CAUTION: The power supply cord plug serves as the main disconnect for the product. The socket-outlet shall be installed near the product and be readily accessible.
CAUTION: Voltages present which are above TNV-3 (POTS) limits. A cover must be installed over the punch down blocks with a HV (High Voltage) warning label (supplied).

The maximum operating ambient temperature is 50 degrees Celcius.

When installing the Switch in an equipment rack, consider the following potential hazards:

Elevated Operating Ambient Temperature – If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra).
Reduced Air Flow – Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
Mechanical Loading – Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
Circuit Overloading – Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
Reliable Earthing – Reliable earthing of rack-mounted equipment should be maintained.
Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

m2 WallPlate
CAUTION: Use only power supplies listed in the user manual
When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.

SAVE THESE INSTRUCTIONS

Waste Electrical and Electronic Equipment (WEEE)

English: For EU Customers: All products at the end of their life must be returned to Motorola for recycling. For information on how to return product, please go to: www.motorola.com/recycling/weee.

Bulgarish: За клиенти от ЕС: След края на полезния им живот всички продукти трябва да се връщат на Motorola за рециклиране. За информация относно връщането на продукти, моля отидете на адрес: www.motorola.com/recycling/weee.

Dansk: Til kunder i EU: Alle produkter skal returneres til Motorola til recirkulering, når de er udtjent. Læs oplysningerne om returnering af produkter på: www.motorola.com/recycling/weee.

Deutsch: Für Kunden innerhalb der EU: Alle Produkte müssen am Ende ihrer Lebensdauer zum Recycling an Motorola zurückgesandt werden. Informationen zur Rücksendung von Produkten finden Sie unter: www.motorola.com/recycling/weee.

Eesti: EL klientidele: kõik tooted tuleb nende eluea lõppedes tagastada taaskasutamise eesmärgil Motorola'ile. Lisainformatsiooni saamiseks toote tagastamise kohta külastage palun aadressi: www.motorola.com/recycling/weee.

Español: Para clientes en la Unión Europea: todos los productos deberán entregarse a Motorola al final de su ciclo de vida para que sean reciclados. Si desea más información sobre cómo devolver un producto, visite: www.motorola.com/recycling/weee.

Français : Clients de l'Union Européenne : Tous les produits en fin de cycle de vie doivent être retournés à Motorola pour recyclage. Pour de plus amples informations sur le retour de produits, consultez: www.motorola.com/recycling/weee.

Italiano: per i clienti dell'UE: tutti i prodotti che sono giunti al termine del rispettivo ciclo di vita devono essere restituiti a Motorola al fine di consentirne il riciclaggio. Per informazioni sulle modalità di restituzione, visitare il seguente sito Web: www.motorola.com/recycling/weee.

Magyar: Az EU-ban vásárlóknak: Minden tönkrement terméket a Motorola vállalathoz kell eljuttatni újrahasznosítás céljából. A termék visszajuttatásának módjával www.motorola.com/recycling/weee.

Nederlands: Voor klanten in de EU: alle producten dienen aan het einde van hun levensduur naar Motorola te worden teruggezonden voor recycling. Raadpleeg www.motorola.com/recycling/weee voor meer informatie over het terugzenden van producten. www.motorola.com/recycling/weee.

Português: Para clientes da UE: todos os produtos no fim de vida devem ser devolvidos à Motorola para reciclagem. Para obter informações sobre como devolver o produto, visite: www.motorola.com/recycling/weee.

Românesc: Pentru clienții din UE: Toate produsele, la sfârşitul duratei lor de funcționare, trebuie returnate la Motorola pentru reciclare. Pentru informații despre returnarea produsului, accesați: www.motorola.com/recycling/weee.

Slovenski: Za kupce v EU: vsi izdelki se morajo po poteku življenjske dobe vrniti podjetju Motorola za reciklažo. Za informacije o vraèilu izdelka obišèite: www.motorola.com/recycling/weee.

Suomi: Asiakkaat Euroopan unionin alueella: Kaikki tuotteet on palautettava kierrätettäväksi Motorola-yhtiöön, kun tuotetta ei enää käytetä. Lisätietoja tuotteen palauttamisesta on osoitteessa: www.motorola.com/recycling/weee.

Svenska: För kunder inom EU: Alla produkter som uppnått sin livslängd måste returneras till Motorola för återvinning. information om hur du returnerar produkten finns på www.motorola.com/recycling/weee.

Commands and Syntax **8**
Command Hierarchy 8
Administrative Commands 8

Hardware **10**
Model Numbers and Description 10
Switch Front Panel Connections 11
Mounting Options 11
Switch Rear Panel Connections 11
WallPlate 12

System Administration **13**
Management Access 13
CLI Configuration Script files 13
Configuration Files using the webUI 14
HTTP Menus 15
Upgrading the System Image 15
Line Quality 15
View System Configuration and Status 16
Commit mode 16
Reset to Default Configuration 17
Other Configuration Help 17

Access Control Lists (ACLs) **18**

RADIUS network authenticated login **19**

WallPlate Installation **20**
Installation Guidelines 20
Installation 1: Install over 70mm x 114mm wall plate 21
Installation 2: Install over European wall plate with 65mm offset 22
Installation 3: External mounting tabs 23
Remove the cover to service the WallPlate 23

Installation Steps **24**
Install mT2 switch in phone room; MDF or IDF 24
Install cross connects 24
Review the cross-connects 24
Configure mT2 EthernetXD Switch 25
In-Room Installation 26
Enable line power 28
Finish the installation 28

802.1Q VLANs **29**
VLAN Specification 29

VLAN terminology 29
VLAN commands in mT2 30
Web UI configuration 31

Quality of Service (QoS) 34
QoS commands and concepts 34
Dynamic packet classification 36

QoS Example 37

VLAN Tutorials 38
Tutorial 1: Simple Hotel configuration 38
Tutorial 2: Mixed Mode VLAN configuration with QoS 39
Tutorial 3: Per port 802.1Q VLANs 41
Tutorial 4: Network Privacy without 802.1Q VLANs (cascade optional) 43

Line Status 45

Appendix A: Pin-out Assignments 47

Appendix B: Hardware Specifications 49

Appendix C: Compliance 51

Commands and Syntax

Command Hierarchy

The Tut Command Line Interface (CLI) implements a hierarchical command structure. Commands are organized as a high-level command keyword related to a particular function of the device with sub-commands related to sub-functions.

You may move down in the command hierarchy by entering root keywords and sub-keywords followed by the enter key. Your current level in the command hierarchy is referred to as the "command context." The top-level context is referred to as the "root command context." You may move up to the previous command context by using the exit command. The command prompt displays the current command context.

Full commands may be entered at the root command context. For example:

```
system> interface dsl enable port1
```

You may also move down levels in the command hierarchy, which allows you to execute commands with less repetitive typing.

For example:

```
system> interface
system:interface> dsl
system:interface.dsl> enable port1
system:interface.dsl> enable port2
system:interface.dsl> enable port3
system:interface.dsl> exit
system:interface> exit
system>
```

Administrative Commands

Most commands discussed in this guide are administrative commands, which change the configuration of the system or affect the operation of the system. These commands can only be executed from the **admin** account. Configuration changes take affect immediately and are recorded in non-volatile memory (NVRAM) in the default mode. Alternatively, you may choose not to record changes in NVRAM. In this case, changes will need to be committed before rebooting the system; otherwise the configuration will revert to the last saved configuration. If automatic commit is enabled, or the configuration is manually committed, the running configuration will automatically be restored if the system power cycles or is rebooted.

Show Commands

The **show** commands are used to view configurations, status and/or statistics. These commands can be issued from either the **user** or **admin** account.

Global Commands

Commands that are available from any command context are called *global* commands. For example, the **help** command can be used whether you are at the root command context or down a few levels in the command hierarchy. Global commands can also be used from either the **user** or **admin** account.

> **Note:** The default prompt is "system>". If you set the system name using the "**system name**" command, the prompt changes to the new system name.

Command	Description
clear	Clears the screen
exit	Use this command to switch to the previous context. Note that using the **exit** command at the root command contgext performs the same function as logout.
help	Displays the help files
history	Shows the history of the commands used in the current session.
logout	Can be used with either the login (admin, user, RADIUS network authenticated) and at any command level to terminate the current session
tree	Shows the structure of the command tree

Command Completion

The Tut OS allows you to shorten commands as long as the characters are not ambiguous. While typing a command, press the tab key to have the system complete the current command word or type (**?)** to have the system display a list of available options. The options displayed vary according to the context:

• If you type a **?** at a prompt, the system displays a list of all available commands.
• If you type an unambiguous command word, pressing **?** displays all available subcommands or arguments. For example, **show ?** (note the space before the question mark) displays a list of all show subcommands.

Style Conventions

The style conventions used in this manual distinguish various elements of the commands and facilitate the proper interpretation of command syntax, parameters, and their use.

This document refers to actual command syntax as little as possible. For a complete command syntax document, please refer to the *Command Reference* guide for a complete list of all available commands, the proper syntax, and usage examples. In no way does this User Guide attempt to replace or obsolete the *Command Reference*.

Interface Range

Multiple interfaces can be specified for a single command using port ranges. Use of hyphens (-) and commas (,) to delineate ports. Port numbers must be contained in parenthesis. Hyphens and commas can be combined in the same expression to specify multiple, non-sequential interfaces. For example;

To enable all 25 DSL ports, type: *interface dsl enable port(1-25)*

To enable only selected DSL ports, type: *interface dsl enable port(1,3,5,20-25)*

Hyphens and commas can also be used to enable remote Ethernet ports along with DSL ports. For example;

To enable Eth1 and Eth3 on every WallPlate, type: *interface remote enable port(1-25)-(1,3)*

VLAN commands can also be completed using interface ranges.

To add VLAN 100 to Eth1 on every WallPlate, type: *vlan membership add 100 interface port(1-25)-1*

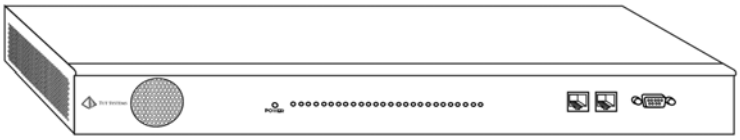
Hardware

Model Numbers and Description

Model Number	Description
45025	25 port mT2a Ethernet^{XD} Switch. 2 x GigE uplink Ethernet ports and 25 x high speed DSL ports for connection to UTP wiring. Provides broadband data and Adaptive Line Power for remote WallPlate.
45125	RoHS compliant version of 45025
45001	2 port m2a WallPlate. 2 x Fast Ethernet ports, 1 x high speed DSL port, 1 x analog POTs RJ11 port. Two powering options; Adaptive Line Power from the 45025 switch, or local power adapter. Designed for installation over existing RJ11 wall jack.
45101	RoHS compliant version of 45001
45003	4 port m4a WallPlate. 4 x Fast Ethernet ports, 1 x high speed DSL port, 1 x analog POTs RJ11 port. Two powering options; Adaptive Line Power from the 45025 switch, or local power adapter. Designed for installation over existing RJ11 wall jack. RoHS compliant.
45002	4 port m4 Service Unit. 4 x Fast Ethernet ports and 1 x high speed DSL port. Two powering options; Adaptive Line Power from the 45025 switch, or local power adapter. Analog POTS filter and port is not included. Solid backplate, not designed for installation over existing RJ11 wall jack. RoHS compliant.
65601	In-line RJ11 filter, mT2a. RoHS compliant
65602	In-line unterminated filter, mT2a. RoHS compliant
65002	12VDC regulated power supply, US. RoHS compliant
65102	12VDC regulated power supply, Euro. ROHS compliant
61299	RJ11 telephone cable, 2m. RoHS compliant

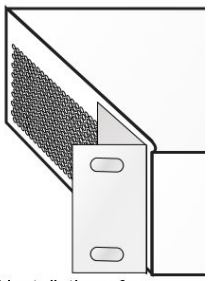
Switch Front Panel Connections

- ETHERNET PORTS: 2 x 10/100/1000 auto-sensing
- CONSOLE PORT: db9 serial

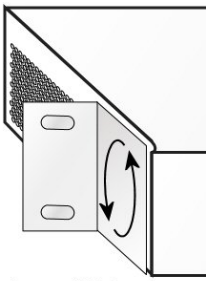


Mounting Options

T2 ships with mounting ears designed for a standard EIA-19 equipment rack. The ears can be rotated 180 degrees.



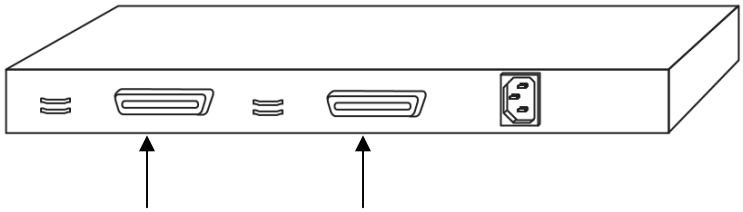
Normal installation of ears
Unit will extend 0mm



Rotate ear 180 deg
unit will extend by 50mm

Switch Rear Panel Connections

- LINE RJ21: PBX/PSTN block or breakout panel
- PHONE RJ21: House block or breakout panel
- POWER: 100-240VAC IEC320 male connector

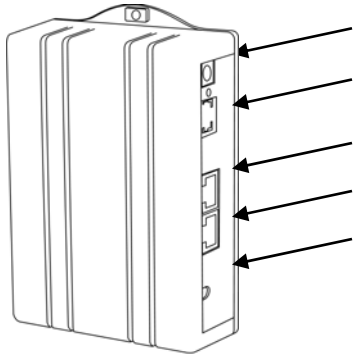


LINE RJ21
Connect to PBX

PHONE RJ21
Connect to House block

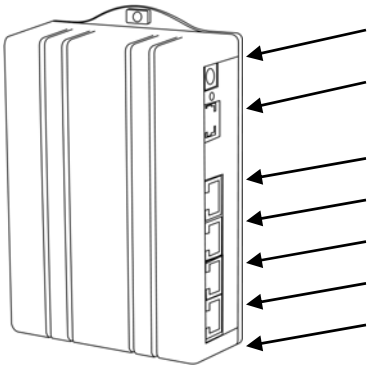
WallPlate

m2a – 2 port WallPlate
Designed to be installed over existing RJ11 wall jack. Bracket has a large opening to route the RJ11 cable from the existing jack. See Installation Chapter for a breakout view of the cover and bracket.



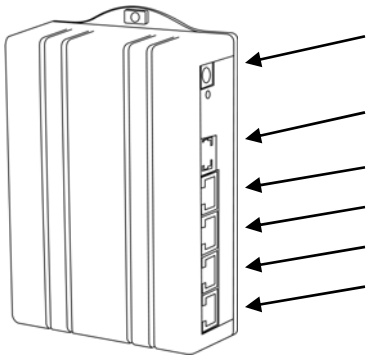
DC power connector (not used from 0 to 600meters)
RJ11 filtered phone port
Eth1 – 10/100 auto-sensing Ethernet
Eth2 – 10/100 auto-sensing Ethernet
RJ11 line-in port (not shown, accessible when bracket is removed)

m4a – 4 port WallPlate
Designed to be installed over existing RJ11 wall jack. Bracket has a large opening to route the RJ11 cable from the existing jack.



DC power connector (not used from 0 to 600meters)
RJ11 filtered phone port
Eth1 – 10/100 auto-sensing Ethernet
Eth2 – 10/100 auto-sensing Ethernet
Eth3 – 10/100 auto-sensing Ethernet
Eth4 – 10/100 auto-sensing Ethernet
RJ11 line-in port (not shown, accessible when bracket is removed)

m4a – 4 port Service Unit
Designed to be set on a shelf, or mounted on flat surface. Not designed for installation over an existing RJ11 jack. The mounting bracket is solid, there is no hole to route an RJ11 cable behind the unit. The line-in RJ11 jack is located on the external side of the unit. The Service Unit does not have an integrated POTS filter.



DC power connector (not used from 0 to 600meters)
RJ11 line-in port
Eth1 – 10/100 auto-sensing Ethernet
Eth2 – 10/100 auto-sensing Ethernet
Eth3 – 10/100 auto-sensing Ethernet
Eth4 – 10/100 auto-sensing Ethernet

System Administration

This User Guide does not detail each configuration command option. Consult the mT2 Command Reference for an alphabetical listing of all commands, proper syntax, and examples.

This chapter covers common management questions and items not covered by the Command Reference.

Web UI context-sensitive help includes information on each configuration item.

Management Access

mT2 can be managed via serial console, telnet, HTTP web UI, or SNMP. With the 1.3 firmware, Eth1 is enabled by default. Telnet and HTTP are accessible at the default IP address.

Access Methods

Default IP address	192.168.1.3
Serial console	Terminal settings: 9600-8-N-1 no flow control
Telnet	Requires Eth1 or Eth2 enabled and a valid IP address
HTTP	Requires Eth1 or Eth2 enabled and a valid IP address Browser support: IE6 or greater, Mozilla Management URL: http://<IP address>

Default login and password

Default user name for administrative access: admin
Default password: <blank>

Default user name for monitoring only: user
Default password: <blank>

CLI Configuration Script files

With the 1.3.0 firmware release, T2 features a 200 kbyte file system to store and load configuration script files. These files are text editable. Use the following commands to complete these management tasks:

1. Create a starting configuration file from an existing T2 unit
2. Copy the file to an external server
3. Edit the file on a PC
4. Load the file into another T2 unit
5. Execute the file as a set of configuration commands

The command syntax to use the file system is:

file copy <string(source)> to <string(destination)>

a. Source can be a local file, a remote FTP or TFTP file, or a pre-defined keyword. Keywords allow you to capture the startup and running configuration to a file. Supported keywords are “startup” and “running”.

b. Destination can be a local file or a remote FTP or TFTP file. Note that the combination of the Source keywords and the remote Destination allows you to copy the running config directly to a remote server. For example; file copy running to tftp://192.168.1.1/my-t2-config.txt

c. At least one (source or destination) must be the local file system. If the source and destination are remote servers, the command will fail.

file delete <string(file)>

d. Delete a file from the file system

file dir

e. List the files in the system and display the remaining storage

file exec <string(file)>

f. Executes a file as a set of configuration commands. Note that “file” is a local file in the file system. The file must have previously been copied to the filesystem from the external server using the ***file copy*** command.

Configuration Files using the webUI

From the webUI, the administrator can save and load configuration files. Note that these configuration files are non-editable binary format for configuration security. If editable configuration is desired, use the CLI script files. Configuration files from the webUI can be used to create secure template configurations.

Note: The Configuration File contains every configuration possible including the “Admin” account password. When combined with RADIUS network authentication, the non-editable Configuration Files provide a secure method to pre-configure systems in a staging area and apply the secure “admin” password without revealing the password. Contact a Tut Systems support person for assistance with a setting up secure, staged configurations.

To save or load a Configuration file from the webUI, access the **System – Configuration** screen from the webUI.

Follow these steps to create a template configuration file:

1. Configure a complete system configuration
2. Set the system name to “template configuration” or similar name
3. Save the configuration file using the webUI System-Configuration screen

Follow these steps to apply the template to a new system:

1. Boot a new system
2. Using the serial console login, set the IP address (or use the default IP address)
3. Reboot the system to apply the IP address
4. Login via the webUI
5. Load the template configuration file using the System-Configuration screen
6. Change the system name to the correct name
7. Change the IP address to the correct IP address
8. Power off or reboot the system. The next time the system is booted, it will have the complete configuration with the correct IP address and system name.

HTTP Menus

System Menu	All configuration items related to setting up the system and management access. For example; IP address, SNMP, image upgrade
Interface Menu	Ethernet and DSL port configuration
Advanced Menu	VLAN, IGMP, advanced configurations
Monitor Menu	Quick access to all port statistics; line quality, etc

Color coded Port Monitor:

- Green - Ethernet Port or DSL Port is operating normally and within tolerance
- Gray - Ethernet Port is enabled, but disconnected.
- Yellow - Indicates an alert condition.
- Red – Indicates a warning or alert condition. When applied to the Line Status, Red indicates the line is enabled, but the WallPlate is disconnected.
- Black – Port is disabled

Upgrading the System Image

MT2 stores one active and one alternate boot image.

The WallPlate software image is included with the mT2 system image. At bootup, the image is checked for current version and any required changes. If the WallPlate image requires a reload (as during a system image upgrade), the time to upload all 25 WallPlates is approximately 20 minutes. During the upgrade time, the WallPlates will not be available for network activity. Currently, there are no WallPlate upgrades planned for current releases of mT2 software.

System image can be upgrade using FTP or TFTP. Commands used are:

Using FTP: *system image load ftp://username:password@ipaddress/path/t2-app.img*
Using TFTP: *system image load tftp://ipaddress/path/t2-app.img*

Instructions to obtain and upgrade the system image are found in the release notes of each software image.

Line Quality

mT2 includes Forward Error Correction in the VDSL frames. Bit errors that are not corrected are counted and reported as a Line Quality measurement. Bit errors are averaged over 1 second of time. An SNMP trap will be sent to the SNMP trap recipient when the threshold is crossed. The line quality status will change in the webUI and the Command Line Interface. There are two thresholds that will be set:

Maximum threshold – the line quality status will change to Fair when the errors increase beyond the maximum threshold

Minimum threshold – the line quality status will change to Good when the errors decrease below the minimum threshold

To set the line quality threshold, use the following command:

interface dsl threshold <interface-id> min-threshold <0.5 to 50> max-threshold <0.5 to 50>

Line quality threshold can also be set from the webUI using the **Interface DSL** menu

By default, the thresholds are set to:

min-threshold 1.7 bit errors/second
max-threshold 2 bit errors/second

View System Configuration and Status

Configuration and Status can be viewed using the Show commands. To view all the options to display configuration and status, use the following command from the CLI:

show ?

Ex: View Current and alternate software versions:

show system image

XLT displays the configuration from the CLI in three useful modes. All configuration displays can be accessed from the "show system config" command syntax.

Summary	Use the command: *show system config summary* This command displays the configuration in an organized summary of each configured feature. Use this output to quickly view the active configuration.
Startup	Use the command: *show system config startup* Displays only the commands entered by the administrator that result in a configuration change AND have been saved to memory. Use this command to capture an active configuration and create a template for configuring other XLT switches.
Running	Use the command: *show system config running* Displays only the commands entered by the administrator that result in a configuration change. The changes may or may not have been saved to memory. Use this command to capture an active configuration and create a template for configuring other XLT switches. **Note:** When the commit mode is set to manual, the Running config will be different from the Startup config until the changes are committed.

Commit mode

Tut OS supports automatic and manual commit modes. When in automatic mode, every command will be executed immediately and saved to memory. The commands will be active if the system is rebooted or power cycled.

In manual mode, commands are executed immediately, but are not saved to memory. The commands will be lost when rebooted if they are not committed.

To change the mode:

system config mode <*auto*|*manual*(mode)>

To commit manual commands to memory:

system config commit

Reset to Default Configuration

From the CLI, enter the following command:

system config default

Note: This command is only available from a local serial login session.

Other Configuration Help

The *mT2 Command Reference* is the master text for all T2 configurations. It contains an alphabetical listing of all CLI commands, syntax and example configuration.

The web UI features a context-sensitive help system.

Access Control Lists (ACLs)

The Tut OS provides layer 3 ACLs based on an administrator defined IP addresses and pre-defined services. The pre-defined services are HTTP, FTP, Telnet, SNMP. The Tut OS ACLs supports 10 indexed entries. Each index entry can contain an IP address, pre-defined service, or combination of IP address and service.

ACLs are processed from index 1 through index 10. If no matches are found, the access is granted.

Place the most restrictive access rules on the lower index number.

To enter ACLs from the CLI, use the following command:

ip access-list config <*1-10*(index)> <*deny*|*permit*(type)> [**ip-address** #.#.#.#] [**mask** #.#.#.#] [**service** *all*|*ftp*|*telnet*|*http*|*snmp*]

Ex: To block all HTTP access from any device, enter:

ip access-list config 1 deny http

Ex: To block all network access from all devices except Telnet from a specific subnet, enter:

ip access-list config 1 permit ip-address 64.174.72.129 mask 255.255.255.128 service telnet
ip access-list config 10 deny service all

Note: A 32-bit subnet mask will specify one single device with the specified IP address

RADIUS network authenticated login

XLT will authenticate network logins from user accounts and passwords maintained on a remote RADIUS server. XLT implements RADIUS access-requests. RADIUS network authenticated logins allows the administrators to easily change all passwords by changing the password on the RADIUS server, simplifying management of a large network with multiple users.

Some RADIUS servers can authenticate using Microsoft Active Directory; thus network logins can be tied to the technicians network login account. Using this method, password management is tied directly to the users network authentication.

To use RADIUS network authentication, you will need a properly configured RADIUS server (free RADIUS servers are available for Linux operating systems or fee-based server products are available on UNIX and Microsoft NOS).

RADIUS authenticated logins only support the “admin” user account privileges with the following exceptions:

- The RADIUS account cannot disable RADIUS login support
- The RADIUS account cannot change the built-in “Admin” password

To create a RADIUS server configuration from the CLI, use the following command:

radius server config <*1-5*(index)> <**ip-address** #.#.#.#> <**shared-secret** *string*> <**timeout** *1-10*> <**retries** *1-120*>

Options	Description
index	5 RADIUS servers can be added. Authentication will be performed starting with the server in index 1
ip-address	IP address of the RADIUS server
shared-secret	This is the password used by the RADIUS server to authentication the Access-Request packets from the Tut OS
timeout	Number of seconds to wait after sending an Access-Request packet before sending another request or trying another server. Practical timeout value is 5 seconds.
retries	Number of retries before giving up and trying a different server. A practical entry for retries is 2 to 3.

Note: The “admin” account name is not reserved. You may create an “admin” account on the RADIUS server. If so, the Tut OS will first check the password against the local “admin” account password before trying the RADIUS server. Unless there is a special reason to do so, we recommend not using an “admin” account on the RADIUS server.

WallPlate Installation

Installation Guidelines

The WallPlate must be anchored to a structurally stable surface. Flexible mounting options allow the WallPlate to be installed onto an existing telco box, or on a wall.

Mounting options for existing telco box

1. Using the keyhole slots; mount over a 70mm x 114mm telephone wall plate as found in North America, South America, Asia-Pacific.
2. Using the horizontal slots; mount over a telephone wall plate with 65mm offset mounting screws. Most European telephone wall plates have 65mm offset mounting screws.

Other mounting options

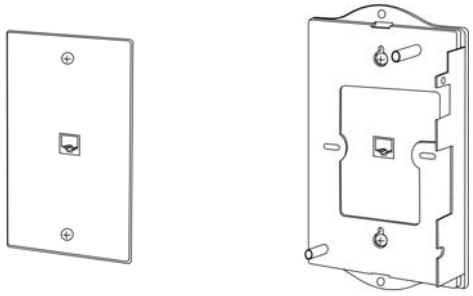
When the above option is not possible; mount the m2a to a flat surface using the external mounting tabs.

If installing the WallPlate on a wall with gypsum board (sheet rock, drywall); use 50mm long wood screws to attach the WallPlate to the wall studs. Do not install the WallPlate to gypsum board unsupported.

Installation 1: Install over 70mm x 114mm wall plate

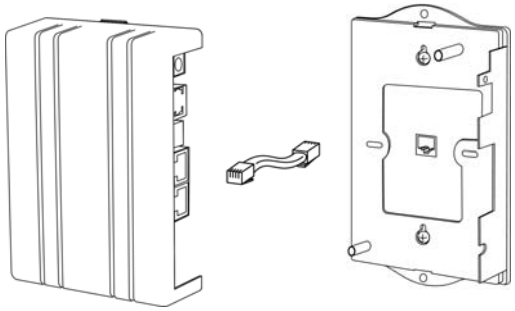
Step 1: Install bracket over existing wall plate

1. Loosen retaining screws on the existing RJ11 wall plate
2. Align bracket keyhole slots over retaining screw heads
3. Slide bracket over retaining screws
4. Tighten retaining screws to affix bracket to RJ11 wall plate



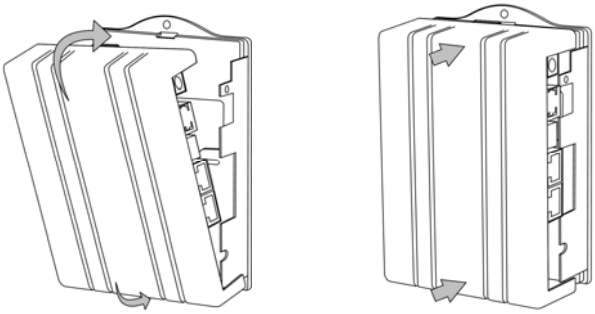
Step 2: Install RJ11 line cable

5. Connect short RJ11 pigtail cable to internal RJ11 connector on the m2a circuit board
6. Connect other side of RJ11 pigtail cable to RJ11 connector on the RJ11 wall plate



Step 3: Attach cover to the bracket

7. Use a slight angle to align the bottom connector.
8. Apply firm pressure to the top and bottom of cover to snap the connectors in place.
9. Install two (2) set screws in the pre-drilled holes in the top of the cover.



Installation 2: Install over European wall plate with 65mm offset

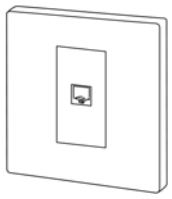
The European style wall plate is comprised of four primary parts; the box, the modular connector, mounting bracket for the modular connector, and the outer plastic cover. The decorative plastic cover can be discarded and replaced by the m2a WallPlate.

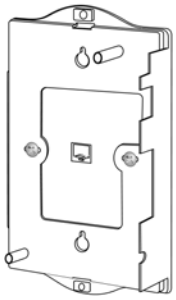
Variance from Country to Country

1. Typical dimensions of the telco box are 70mm square; 85mm square, or 90mm square with a 65mm mounting screw offset.
2. Existing mounting screws are typically 5mm to 10mm. Check local machine screw dimensions and thread style when planning the installation. Typical required length is 10mm to 20mm. Replacement machine screws should be obtained locally prior to the installation.

Step 1: Remove and discard cover over existing wall plate

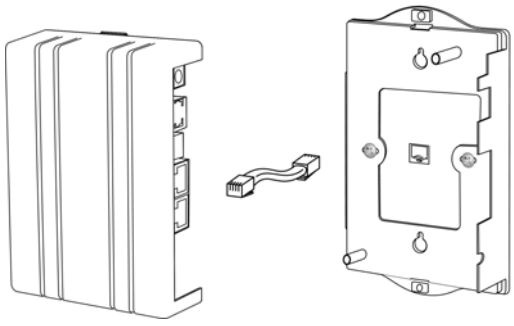
3. Remove plastic cover and expose RJ11 bracket and mounting screws
4. Remove mounting screws
5. Align bracket horizontal slots over 65mm offset mounting holes
6. Install mounting screws (replace with 20mm machine screws if necessary)





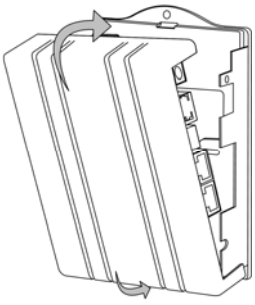
Step 2: Install RJ11 line cable

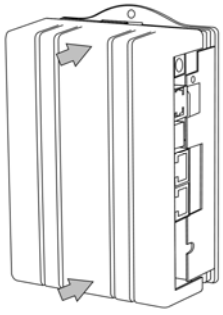
7. Connect short RJ11 pigtail cable to internal RJ11 connector on the m2a circuit board
8. Connect other side of RJ11 pigtail cable to RJ11 connector on the RJ11 wall plate



Step 3: Attach cover to the bracket

9. Use a slight angle to align the bottom connector.
10. Apply firm pressure to the top and bottom of cover to snap the connectors in place.
11. Install two (2) set screws in the pre-drilled holes in the top of the cover.





Installation 3: External mounting tabs

If the first two Installation methods are not possible e.g. European box mounted externally on the base molding or other surface, then mount the m2 WallPlate using the external mounting tabs.

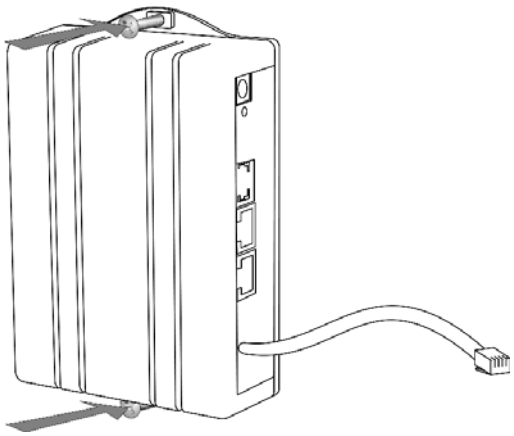
NOTE: Order the RJ11 long cable assembly from Motorola PBN. Part number 61299

Step 1: Connect RJ11 cable

1. Connect 2m cable (Tut p/n 61299) to the internal RJ11 connector on the m2a circuit board
2. Route the RJ11 cable out of the bracket using the exit hole next to the Ethernet ports

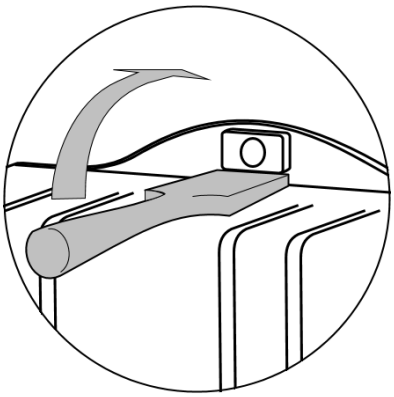
Step 2: Assemble the m2 WallPlate

3. Snap the cover and bracket together
4. Install WallPlate unit to the wall or structurally sound flat surface using the external mounting tabs.



Remove the cover to service the WallPlate

1. Remove the two (2) set screws in the top of the cover.
2. Insert a flat blade screwdriver between the bottom tab and the m2a cover
3. Apply a prying motion as shown to loosen the bottom hook on the m2a cover
4. Repeat the steps on the top tab of the m2a cover



Installation Steps

PLEASE READ

mT2 features Adaptive Line Power (ALP) for the WallPlates. Follow these instructions when installing the mT2 system. Note that line power is **not enabled** until after a successful link using an external power supply. Consult the Appendix for Electrical Safety Information.

PLEASE READ

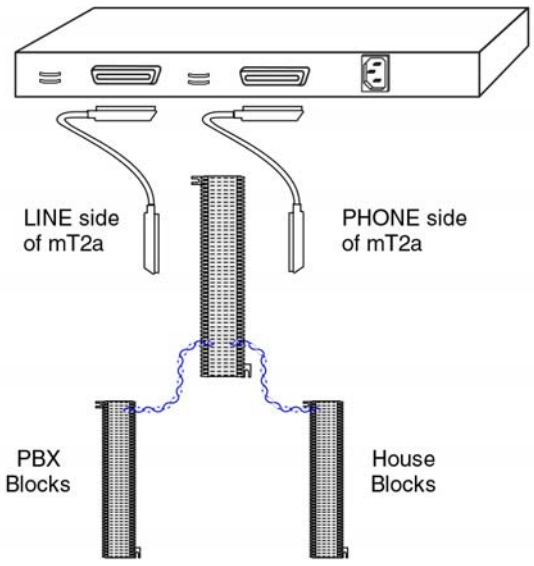
The following instructions assume knowledge and skills with installing xDSL systems. The details below are relevant to the mT2 installation. This is not intended to be a step by step training guide. Please consult your Motorola PBN sales representative if you require training in the installation steps.

Install mT2 switch in phone room; MDF or IDF

1. Install mT2a to equipment rack using the rack-mount ears provided
2. Connect the AC line cord to the IEC320 male receptor on the rear of the unit

Install cross connects

3. Siemens S66M2-5W-TP is the recommended cross connect block. Note the "TP" on the part number.
4. Connect the LINE side mT2 RJ21 to the **left** side of the S66M2-5W-TP block using a M/M RJ21 telco cable
5. Connect the PHONE side mT2 RJ21 to the **right** side of the S66M2-5W-TP block using a M/M RJ21 telco cable
6. Cross-connect line one of each room.
    - Wire pair from the PBX is connected to the **left** side of the block
    - Wire pair from the House is connected to the **right** side of the block



Review the cross-connects

Before proceeding to the configuration and in-room installation, review the cross-connects to ensure:

7. No pairs are split, or double-punched
8. Only line 1 of each room is connected
9. Install HV label (supplied) to punch block cover

Configure mT2 EthernetXD Switch

Initial configuration should be done connected to one of the Ethernet ports on the upstream side of the switch.

Login using a serial console connection, telnet or HTTP. Note the default IP address of the unit if using a network login for the initial configuration. Default IP: 192.168.1.3

Enter these commands at the system prompt:

Login with default username and password

Username: admin
Password: <blank>

Assign IP address to unit

ip config ip-address 192.168.20.2 mask 255.255.255.0 gateway 192.168.20.1

Enable Ethernet ports

interface Ethernet enable eth2
system reboot

Enable all High Speed DSL ports

interface dsl enable port(1-25)

Configure all High Speed DSL ports

interface dsl config port(1-25) max-down 100 max-up 10

Enable remote Ethernet port 1 of each WallPlate

interface remote enable port(1-25)-1

In-Room Installation

Note: These instructions follow the **Installation 1** procedure from the previous chapter. Please consult ***WallPlate Installation*** for variations of the installation routine.

Tools Required:

Number 2 Philips head screwdriver
Number 2 flat blade screwdriver

Components provided with the m2a WallPlate:

1 – m2a WallPlate bracket and cover with circuit board
1 – 150mm (6”) RJ11 pigtail cable
1 – RJ11 blanking plug
2 – Number 6 oval head screws, 0.25”

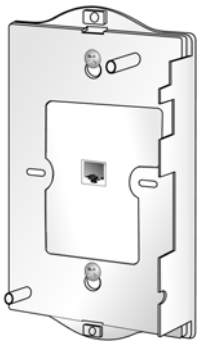
Components required to purchase:

Regulated 12V power supply. Use of the wrong power supply could result in damage to your WallPlate unit. Please order a small quantity of regulated 12V power supplies from Motorola PBN to use during installation.

If you do not have the correct regulated 12V power supply – **STOP**. Order a regulated 12V power supply from your Motorola PBN sales representative.

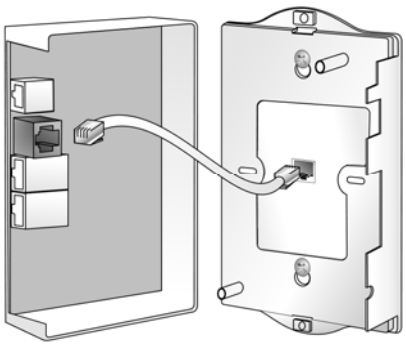
Step 1

1. Loosen screws on wall plate approximately 6mm (1/4”)
2. Attach the bracket using the keyhole slots
3. Tighten screws until the bracket is firmly attached, do not over tighten



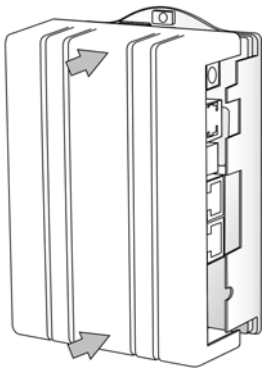
Step 2

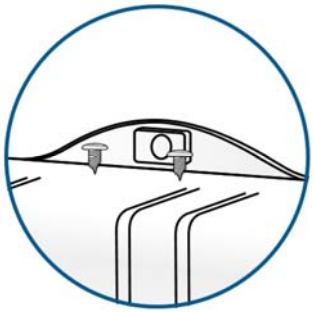
Connect 150mm (6”) cable (supplied) between m2a circuit board and existing RJ11 jack.



Step 3

1. Align bottom hook to bracket using slight angle. Apply firm pressure to top and bottom to snap cover in place.
2. Install two #6 set screws (supplied) in the pre-drilled holes

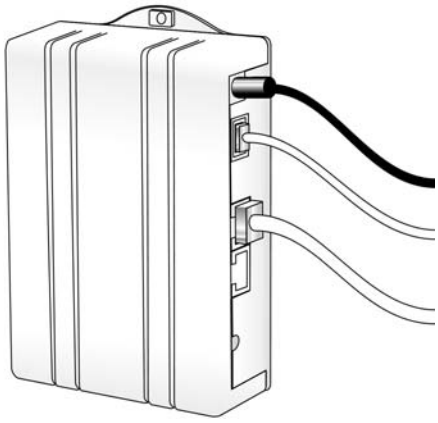




Step 4

1. Connect the local AC power adapter to the WallPlate
2. Connect the analogue phone to the RJ11 phone jack
3. Connect an Ethernet cable (not supplied) to a laptop

The blue LED will flash slow, then fast, to indicate the unit is linking
When the LED stops flashing, the unit is linked



1) AC power adapter used during installation

2) Analog phone

3) Laptop used to test the connection and enable line power

Step 5

After WallPlate blue LED is solid, connect with the mT2 switch using a valid IP address and HTTP or telnet

Enable line power

Login to the mT2 switch using the web UI and HTTP or telnet.

Determine which port is being installed

From the telnet CLI, enter this command:

show bridge address

The MAC address of your PC will appear along with the connected line.

Enable line power

From the telnet CLI, enter this command:

*interface dsl power enable port**x*** (enable only the port being installing)

Finish the installation

Remove the 12V regulated power supply. If the correct port is enabled for line power, the WallPlate will reset and operate from in-line power.

Test the system by connecting to the Internet service provider or other test equipment.

802.1Q VLANs

Note: The system requires a reboot after the “vlan enable” command. If the system is not rebooted, the webUI will not display the VLAN configuration and the CLI will not execute VLAN commands.

Note: VLAN configuration commands have changed with the 1.3.0 firmware release. Older commands are deprecated and will be removed in a future release.

VLAN Specification

VLAN modes:	IEEE 802.1Q standard compliant VLANs or Port-based VLANs on mT2 Switch IEEE 802.1Q standard compliant VLANs on m2 WallPlates
Max number of VLANs:	128
Valid VID range:	1 – 4094
Default PVID:	1
Default Egress:	transmit untagged
Default Ingress:	Accept all packets

VLAN terminology

The T2 Switch is a VLAN switch. The WallPlate is also a VLAN switch. Therefore, be certain that packets traversing the DSL links between the T2 Switch and the WallPlate are always TAGGED.

PVID	In the 802.1Q standard, each port is assigned a PVID. This is the default VLAN ID assigned to ***untagged packets*** received (ingress) on that port. The PVID is sometimes called the port Native VLAN. By default, all ports are assigned VLAN 1.
Tagged	T2 will optionally tag packets when transmitting (egress) on the port. Set the port as a tagged member of the VLAN by using the *vlan membership egress* command. On the T2 Switch, the tag mode of a packet is determined PER VLAN, not per port. By comparison, the Cisco IOS only has a per port setting for tagging. This allows the T2 to support complex VLAN configurations not possible on other switches. On the m2 WallPlate, the tag mode of a packet is determined PER PORT, similar to the Cisco IOS “trunk” mode.
Untagged	T2 will optionally transmit (egress) packets without an 802.1Q VLAN tag. Use Untagged packets on any port that is connected to a non-VLAN aware device. For example; if a PC is connected to the WallPlate ports, packets will be untagged. This is similar to the Cisco IOS “access” mode of a switchport.

Tag-based VLAN Mode	Tag based mode is fully 802.1Q VLAN compliant. You must explicitly configure the Egress and Ingress rules for each port and each VLAN. On the webUI, use the 802.1Q TAG-BASED VLAN menu to configure VLANs. The mT2 Switch and m2 WallPlate can operate independently. Be sure to configure all ports on the Switch and the WallPlates for proper operation. Consult one of the VLAN Tutorials.
Port-based VLAN Mode	Port based VLAN is also called Port Isolation or Port Privacy in other switches. When operating in port-based mode, the T2 Switch will ignore 802.1Q VLAN tags. Port isolation is based on a VLAN Map. On the webUI, use the PORT-BASED menu to see the VLAN Map and change the mapping. See below for more details. ***Note:*** The Switch operates in port-based mode; whereas the WallPlates only operate in tag-based, or disabled. This allows for special case configurations where the WallPlates do all the 802.1Q VLAN tagging, while the Switch maintains port-to-port privacy.

VLAN commands in mT2

All VLAN configurations are also available from the webUI.

vlan config default	Restore VLAN configuration to default
vlan enable/disable	Enable or disable VLAN support. Requires a system reboot after issuing this command.
vlan add	Create or modify a VLAN.
vlan delete	Delete a VLAN Group. Remove all ports that are members of the group before deleting the group.
vlan name	Enter a friendly name for the VLAN
vlan membership add	Add or delete a VLAN from a port. Allows the VLAN to transmit on the port
vlan membership egress	Sets how a VLAN will egress; with a tag or without. By default, packets will transmit untagged unless specified using this command. Note this command does NOT apply to WallPlate ports
vlan membership delete	Deletes a port from a VLAN membership
vlan interface ingress	Ingress command: Assign the PVID for a port. This VLAN ID will be assigned to all packets received *untagged* on this port
vlan interface egress	Set the Egress mode on any CPE port. This command does not apply to mT2 Switch ports
vlan interface igmp	Assign VLAN for IGMP packets
vlan interface mgmt	Assign VLAN for layer 2 security for all management traffic
vlan mode	Set the mode of operation on the Switch and the WallPlates. Options are IEEE 802.1Q tag-based, or Port-based. ***Note:*** WallPlates only support tag-based or disabled.

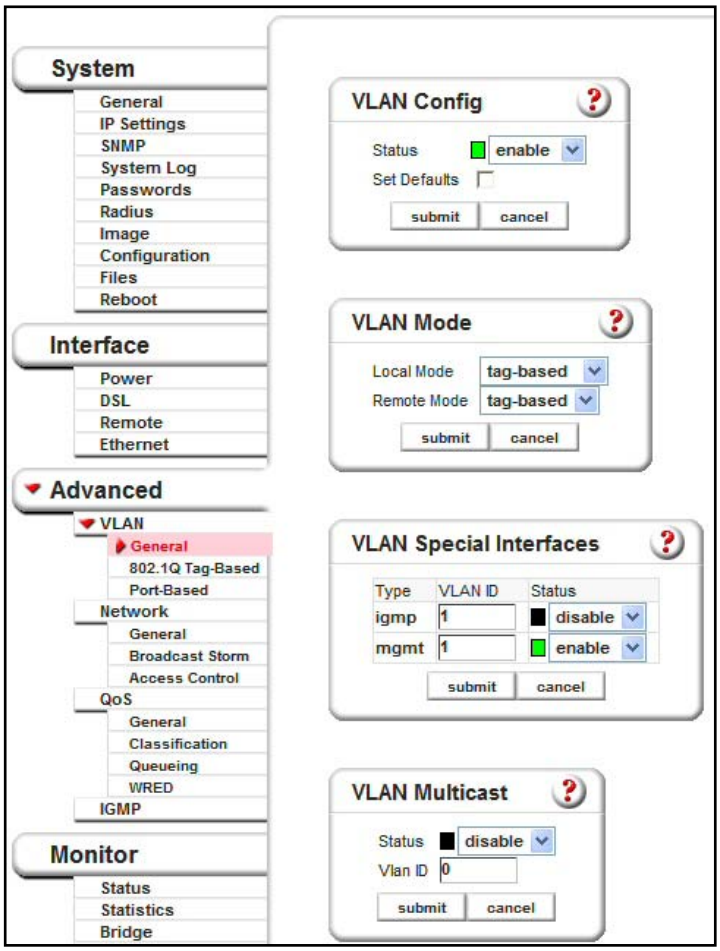
vlan port-group	CLI command to add ports to a Port-based VLAN.
show vlan membership	Displays the memberships in Rows and Columns
show vlan interface	Displays the PVID in Rows and Columns

Web UI configuration

VLANs can be configured from the CLI, web UI or SNMP. The CLI advantage is support for scripting the entire configuration. The CLI disadvantage is the large number of commands required to execute the complete configuration.

The web UI is slower since it relies on Javascript running on your local PC, and the overhead associated with transmitting the configuration data. The graphical display is easy to follow and should be used to get familiar with the system.

Vlan General webUI



VLAN Config
Enable VLAN support. Requires system reboot.

VLAN Mode
Local Mode refers to the mT2 Switch. Port-based or Tag-based is supported. Remote Mode refers to the WallPlate. Tag-based or disabled is supported.

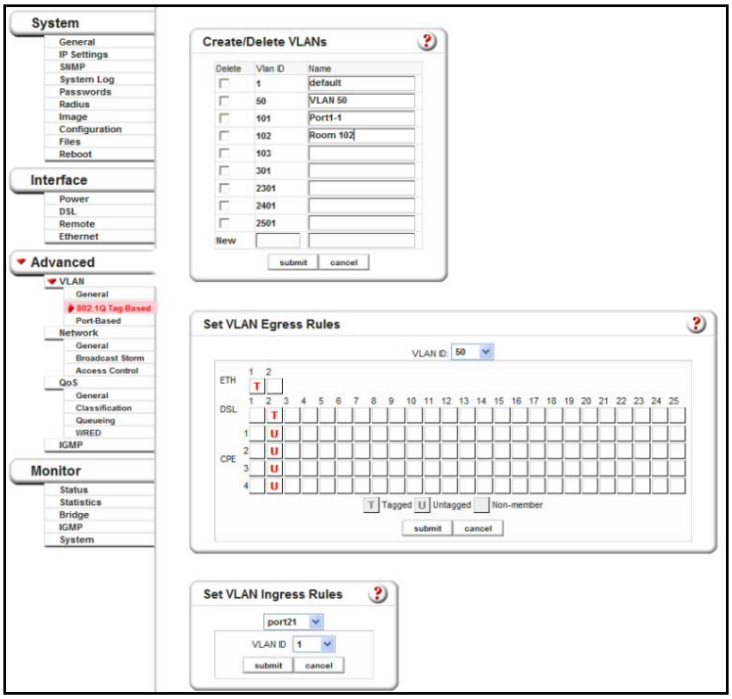
VLAN Special Interfaces
If video is delivered on a defined “video VLAN”, be sure to assign IGMP to the VLAN used for video. When IGMP Proxy is enabled, mT2 will proxy IGMP packets with the VLAN ID of the group in this configuration.

Management packets can be tagged with a specific VLAN ID for layer 2 security. Enable management VLANs and assign a VLAN ID.

The VLAN must first be created using the 802.1Q Tag Based menu.

VLAN Multicast
Enable multicast support and assign the VLAN where multicast packets will be sent. This VLAN should be the same as the IGMP VLAN ID for proper delivery of video.

Tag-based VLAN webUI



Create/Delete VLANs

Use this menu to create new VLANs and assign a name to the VLAN. Note that you cannot delete VLAN 1, however VLAN 1 can be removed from all interfaces.

Set VLAN Egress Rules

Set the VLAN membership rules.
Click 3 times in the box to select (**U**)ntagged, (**T**)agged or not a member. In this example, Eth1 is a (**T**)agged member of VLAN 50.

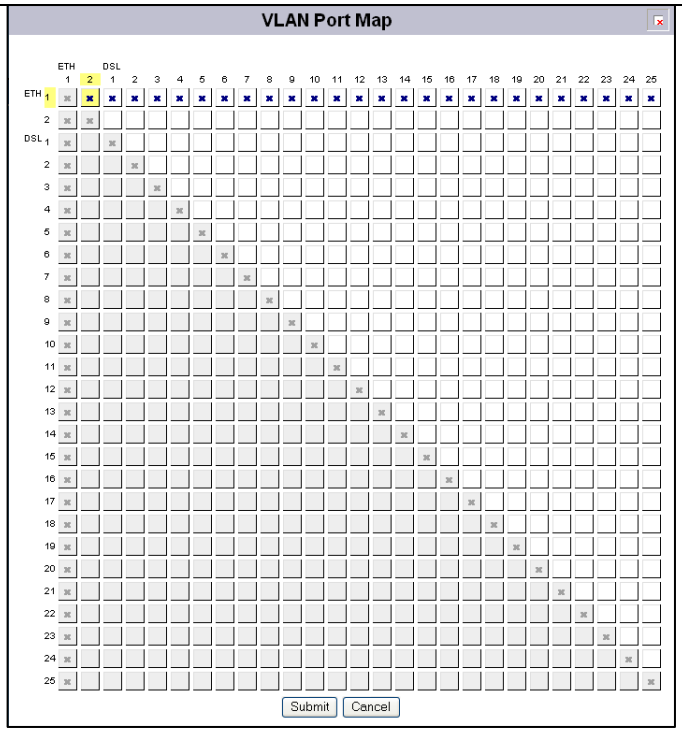
DSL ports will always be a (**T**)agged member of any VLANs on the connected WallPlate

In this example, Port 1 of the first WallPlate is an (**U**)ntagged member of VLAN 50.

Set VLAN Ingress Rules

Set the PVID for each port. This is also known as the native VLAN for the port. All packets received on these ports (as from a PC connected to the port) are assigned the PVID of the port

Port-based VLAN webUI



When the local mode is set to Port-based (The mT2 Switch is the local mode), use the Port-based menu to create a Port Map.

By default, Eth1 and Eth2 can communicate with each other. All DSL ports can communicate with Eth1 and Eth2, but **NOT** with each other.

The example at right shows an effective way to configure port privacy on all DSL ports, and configure Eth2 as a cascade port. This example can be replicated on all Switches in a cascade for simple, effective port privacy.

Note:

- Eth1 can communicate with Eth2
- Eth1 can communicate with all DSL ports
- Eth2 cannot communicate with all DSL ports
- DSL ports cannot communicate with each other

Port-based VLAN webUI, continued

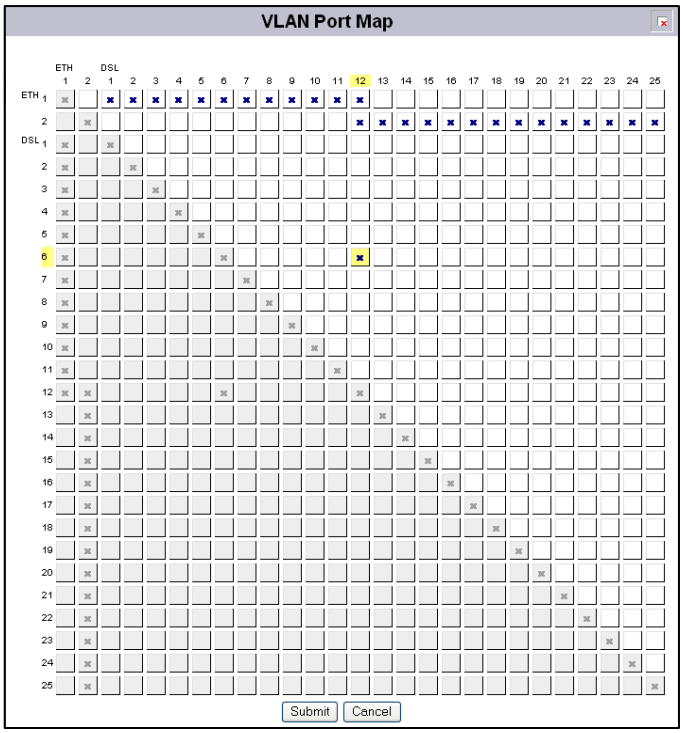
In the example at right, Note:

- Eth1 and Eth2 cannot communicate together
- Eth1 can communicate with DSL ports 1 – 12
- Eth2 can communicate with DSL ports 12 – 25
- Port 12 can communicate with both Eth1 and Eth2
- Ports 6 and 12 can also communicate together

Note that DSL ports can only talk to the upstream Eth1 or Eth2. The only exception is DSL ports 6 and 12.

Port-based mode on the mT2 Switch can be mixed with Tag-based mode on the WallPlate for an effective method to configure VLANs for advanced services.

Note VLAN Tutorial One for an example of mixing Port-based and Tag-based VLANs.



Quality of Service (QoS)

Standards	IEEE 802.1P, WRED, WFQ, IP TOS based on RFC1275
Number of queues	4 queues per port
Packet classifiers	Static classifier: All packets received on a port are assigned to a single queue Dynamic classifier: Packets are assigned to a queue based on their IP TOS or 802.1P
WFQ queue mode	Administrator selectable queue weight. Queue weights are calculated as a percentage of the cumulative weights. Using WFQ, any queue can burst up to the maximum bitrate of the line. This can occur if no packets in a higher priority queue are waiting to transmit. If you wish to apply strict rules and limit a low priority queue to a fixed amount, use the "egress shaping" command.
Priority queue mode	Strict priority over all lower queues. Note that Priority queuing can be mixed with other queuing methods to provide a low latency, low jitter service for sensitive services such as VoIP. For example, if the critical queue were assigned a Priority mode, then those packets would transmit on the port before other packets in the buffers.
Shaping queue mode	Apply traffic shaping rules to individual queues. Each queue is assigned a fixed amount of bitrate. The cumulative bitrate of all the queues should not exceed the total line rate of the port.

QoS commands and concepts

network qos [enable | disable]

Enable qos support. To disable qos, use *network qos disable*

network qos interface priority <interface-id> mode <mode> [level <level>]

Sets the packet classifier mode for the port receiving packets.

Where;

Mode is *dynamic* or *static*. Dynamic classifier will read the IP TOS or 802.1P precedence bit of the incoming packet. Static classifier assigns all packets received on the port to one of the four queues

Level is the default queue for packets received on the port. When the mode is dynamic, then level is assigned to packets that do not match the classifier. When the mode is set to static, then level applies to all packets received on the port.

The four queues are *critical, high, medium,* and *low*.

network qos classification <method>

where **method** is either *802.1p* or *tos*

Once a port has been set to use dynamic or static mode; specify whether T2 will use IP TOS or 802.1P precedence bit for dynamic packet classification.

network qos interface queue <interface-id> mode <mode>

Deprecated commands to set the queuing mechanism on a port. This command is superseded by *network qos interface egress* which has more configuration options.

When using this command, note that WFQ has a fixed percentage for each queue:

Critical: strict priority over all other queues
High: 70% of available bitrate
Medium: 20% of available bitrate
Low: 10% of available bitrate

In priority mode, strict priority applies to all queues where a higher queue always transmits before a lower queue.

Note that when using wfq mode, a low priority queue will use all the available bandwidth if a higher priority queue is not in the transmission buffer.

network qos interface egress priority <interface-id> queue <queue>

Any queue assigned as a Priority queue will transmit using strict priority. A higher level queue will always transmit before a lower level queue. Use priority mode for latency and jitter sensitive applications.

network qos interface egress shaping <interface-id> queue <queue> peak <peak rate> average <avg rate> burst <burst size>

Set a fixed traffic shaping parameter for each queue. Note that a queue will never exceed the peak rate parameter regardless of other services on the port.

Where;

Queue: the queue where you wish to shape traffic. Valid options are critical, high, medium, or low
Peak: the maximum rate for the queue, in Mbits/second
Average: the average rate for the queue, in Mbits/second
Burst: the maximum data burst allowed at the peak rate

network qos interface egress wfq <interface-id> queue <queue> weight <0-200>

Configure the behavior of the WFQ scheduling method. Bitrates are determined as a percentage of the total queue weights.

In order to determine the percentage of bandwidth that will be allocated for a particular queue, divide the queue weight by the sum of all the queues “weight”.

For example; assume the ***High queue*** weight is 100 and the ***Medium queue*** weight is 50. 100 + 50 = 150. So, the High queue will receive 66% of the bandwidth (100/150=0.667) and the Medium queue will receive 33% of the bandwidth (50/150=0.33).

network qos multicast config queue-allocation <allocation>

Multicast packets are allocated a separate set of transmission buffers. Set the multicast queue to be the same queue where the multicast packets will be transmitted. For example, if using video packets with an IP TOS bit, assign the packets to the high queue based on the IP TOS bit, and assign the multicast queue to be also use high. T2 has no way to automatically determine where the multicast packets will be transmitted.

network qos wred enable | disable

Enable or disable WRED support. WRED adds further protection for data integrity in a contention based Ethernet network by randomly discarding TCP packets according to administrator settable parameters for thresholds.

network qos wred config min-discard <min-discard> max-discard <max-discard>

Set the rate at which Ethernet frames will be discarded once the rate exceeds the thresholds. Note that two discard rates are supported. Min-discard is the rate that frames are discarded when they reach the minimum configured threshold. Max-discard is the rate that frames are discarded when they reach the maximum configured threshold. Often, the max-discard rate will be set to 100.

network qos interface wred <eth<1-2>|port<1-25>(interface-id)> <queue low|medium|high|critical> <min-threshold 1-100> <max-threshold 1-100>

Set the minimum and maximum buffer threshold for each queue, on each port. Once either threshold is crossed, frames are discarded at the discard rates specified by the *network qos wred config* command.

Dynamic packet classification

In dynamic mode, packets are classified by the 802.1P Ethernet precedence bit or IP TOS (precedence bits) in the Diffserv byte. This definition is taken from the latest RFC 2475. Note that the IP TOS bits are defined as the three most significant bits of the DiffServ byte.

Ethernet frames are mapped to transmission queues based on the following chart:

802.1P bit	IP TOS	Queue
0	0	Low
1	1	Low
2	2	Medium
3	3	Medium
4	4	High
5	5	High
6	6	Critical
7	7	Critical

QoS Example

An easy way to demonstrate QoS is to use the traffic shaping queue scheduler. To further simplify the example, dynamic packet classifier is not used.

Packet Classification:

Static. All packets on Eth1 will be classified high. All packets on Eth2 will be classified low.

Packet transmission:

Shaping. All four queues will be configured with unique bitrates.

Connections:

A SmartBits network tester can be used; however the same QoS results can be easily demonstrated using iperf and four PCs. In either case, one flow will be connected from Eth1 of the mT2 switch to Port1-1 of the first WallPlate. The other flow will be connected to Eth2 of the mT2 switch and Port1-2 of the first WallPlate.

Commands:

network qos enable
system reboot

network qos interface priority eth1 mode static level high
network qos interface priority eth2 mode static level medium

network qos interface egress shaping port1 queue critical peak 30 average 30 burst 100
network qos interface egress shaping port1 queue high peak 20 average 20 burst 100
network qos interface egress shaping port1 queue med peak 10 average 10 burst 100
network qos interface egress shaping port1 queue low peak 5 average 5 burst 1

Note that the PCs connected to Eth1/Port1-1 will receive 20Mbps bitrate; whereas the other PCs will receive 10Mbps bitrate. While the test is running, change the static level command and watch the behavior change.

network qos interface priority eth1 mode static level low

VLAN Tutorials

Tutorial 1: Simple Hotel configuration

When using a Nomadix subscriber gateway, a special VLAN configuration is required to support unique authentication options for each group of subscribers. For example, in a hotel with both a wired and wireless Internet access, the gateway must use a VLAN ID to identify all users from the wireless network, and a different VLAN ID to identify all users from the wired network. Thus, every user on the mT2 must have the same VLAN ID.

In order to accomplish this, while still maintaining port-to-port privacy, follow this tutorial.

Privacy and QoS in this network:

- Every WallPlate will have the same VLAN IDs
- Privacy enforced between rooms by the port privacy feature on the mT2 switch
- QoS is not used

VLAN-Ids used in this tutorial:

- 100 VLAN used for all wired ports in the network. This VLAN **will transmit** on the upstream network

Third party network configuration:

The mT2 switches will connect to an upstream switch; likely a Cisco or HP. Both these brands offer a port privacy feature that does not rely on 802.1Q VLANs; similar to the function of Port Privacy in the mT2 switch. It is recommended that port isolation be implemented on all aggregation switches upstream of the mT2.

Enable and create VLANs

```
vlan enable
vlan mode local-mode port-based remote-mode tag-based
system reboot

vlan add vlan-id 100
```

Assign the PVID for the WallPlate ports

```
vlan interface ingress port(1-25)-(1-2) pvid 100
```

Assign VLAN memberships to WallPlate ports

```
vlan membership add 100 interface port(1-25)-(1-2)
```

Tutorial 2: Mixed Mode VLAN configuration with QoS

This configuration is designed for dual-service network e.g. VoIP/HSIA or IPTV/HSIA. Each service is assigned an 802.1Q VLAN ID unique for that service. The VLAN tag is used to ensure privacy and QoS throughout the network; from the service provider backhaul to each WallPlate port. In the mT2 system; Port-based VLANs and Tag-based VLANs can be mixed to ensure full port-privacy.

This advantage of this configuration is that it allows the service provider to configure only 2 unique 802.1Q VLAN IDs, and still have guaranteed port-to-port privacy on all ports in the network.

This configuration can be done via the webUI or CLI. The CLI commands are used below.

In this network:

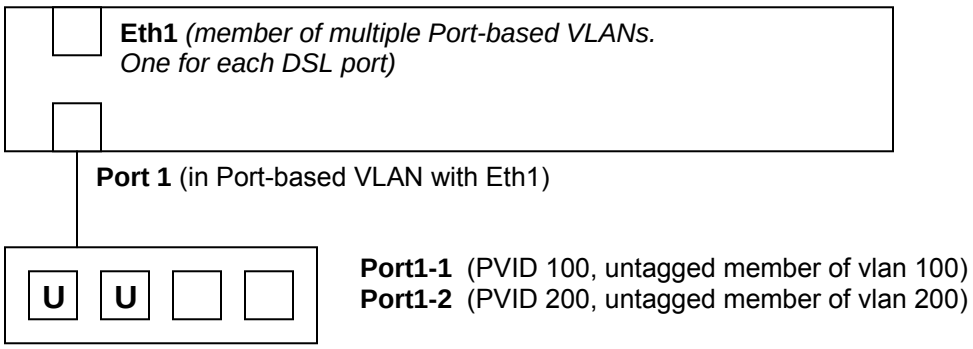
- Low Value Service
    - WallPlate port 1 is connected to a low value service such as HSIA (high speed Internet). All packets are 802.1Q tagged in the mT2 network and transmitted on the core network.
- High Value Service
    - WallPlate port 2 is connected to a high value service such as VoIP or IPTV. All packets are 802.1Q tagged in the mT2 network and transmitted on the core network. QoS is applied in the mT2 based on the 802.1P priority bit.

Privacy and QoS in this network:

- Privacy enforced between high and low value services in the network by the use of two VLAN IDs
- Privacy enforced between WallPlates by using the Port-based VLANs on the mT2 Switch
- QoS critical priority applied to high value service
- High value service packets are tagged with an 802.1P bit of 5

VLAN-Ids used in this tutorial:

- 100 Tag all low value service with this VLAN ID. This VLAN **will transmit** on the upstream network
- 200 Tag all high value service with this VLAN ID. This VLAN **will transmit** on the upstream network



Verify that all devices can ping each other before proceeding

Login to T2 via telnet or hyper-terminal,
From CLI type the following commands:

Enable and create VLANs, Enable QoS

```
network qos enable
vlan enable
vlan mode local-mode port-based remote-mode tag-based
system reboot

vlan add vlan-id 100
vlan add vlan-id 200
```

Assign the PVID for the WallPlate ports

```
vlan interface ingress port(1-25)-1 pvid 100
vlan interface ingress port(1-25)-2 pvid 200
```

Assign VLAN memberships to WallPlate ports

```
vlan membership add 100 interface port(1-25)-1
vlan membership add 200 interface port(1-25)-2
```

Configure QoS for high value service

```
network qos interface priority eth1 mode dynamic level low
network qos classification 802.1p
network qos interface egress wfq port1 queue critical weight 5
network qos interface egress wfq port1 queue high weight 175
network qos interface egress wfq port1 queue medium weight 50
network qos interface egress wfq port1 queue low weight 5
network qos multicast config queue-allocation high
```

Tutorial 3: Per port 802.1Q VLANs

This configuration is designed for a HSIA network where each port 1 on each WallPlate is assigned a unique VLAN.

In this network:

10. WallPlate port 1 is used for HSIA. WallPlate port 2 is disabled to prevent the subscriber from using the wrong port.
11. Eth1 on the switch is connected to an upstream network. Eth2 is disabled.

Privacy and QoS in this network:

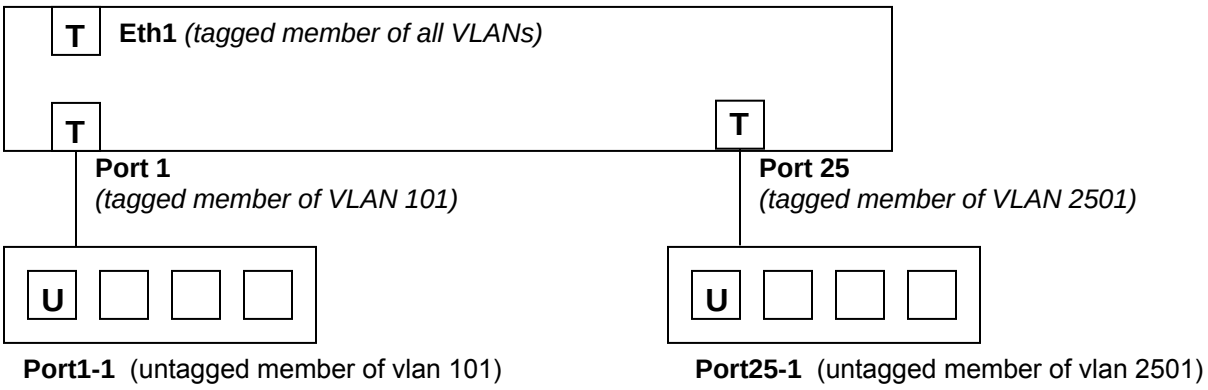
12. Privacy enforced between all ports using 802.1Q VLANs
13. QoS is not used since there is a single service delivered to each user

VLAN-Ids used in this configuration:

14. 101 - 2501 Assigned to port 1 of each WallPlate. The VLAN ID indicates the WallPlate and port number.
15. The chart shows a sampling of VLAN Ids to illustrate the naming convention in this tutorial.

VLAN ID	DSL PORT	ETHERNET PORT
101	1	1
201	2	1
…	…	…
2401	24	1
2501	25	1

16. 4090 This VLAN is assigned as the PVID for Eth1. Since all packets are tagged at all times, this PVID is a place marker to catch untagged packets that may be a security risk.



Verify that all devices can ping each other before proceeding with the following test

Login to T2 via telnet or hyper-terminal,
From CLI type the following commands:

Enable VLANs, configure PVIDs

```
vlan enable
vlan mode local-mode tag-based remote-mode tag-based
system reboot

vlan add vlan-id 4090
vlan add vlan-id 101
vlan add vlan-id 2501

vlan interface ingress eth1 vlan-id 4090
vlan interface ingress port1-1 vlan-id 101
vlan interface ingress port25-1 vlan-id 2501
```

Assign all VLANs to egress on Eth1, configure tagging rules

```
vlan membership add 101 interface eth1
vlan membership add 101 interface eth1

vlan membership egress 101 interface eth1 tag enable
vlan membership egress 2501 interface eth1 tag enable
```

Assign VLAN memberships to DSL ports, configure tagging rules

```
vlan membership add 101 interface port1
vlan membership add 2501 interface port25

vlan membership egress 101 interface port1 tag enable
vlan membership egress 2501 interface port25 tag enable
```

Assign VLAN memberships to WallPlate ports

```
vlan membership add 101 interface port1-1
vlan membership add 2501 interface port25-1

vlan membership egress 101 interface port1 tag enable
vlan membership egress 2501 interface port25 tag enable
```

Convert this tutorial to a real-world configuration

- Create a chart of all VLAN IDs, PVIDs, and membership ports that you require.
    - Pay close attention that the DSL ports are always a tagged port member of a VLAN. Without this step, the VLAN packets will not be able to traverse the DSL lines to each WallPlate.
- Create a configuration script following the command syntax for each step of the tutorial. In the above steps, only VLAN 101 and 2501 are shown. Complete the configuration for all VLANs and ports from 101 to 2501.

Tutorial 4: Network Privacy without 802.1Q VLANs (cascade optional)

This configuration is designed for a secure HSIA network without using 802.1Q VLANs. All WallPlate ports will have VLANs disabled. The mT2 Switch will operate in Port-based VLAN mode. Since VLANs are disabled on the WallPlate, this configuration can be used where all WallPlate ports are in a local, private network. A network printer, network attached storage, or other network device can be connected to Eth1 or Eth2.

Note this configuration is also shown in the webUI examples at the introduction to VLANs earlier in this manual.

In this network:

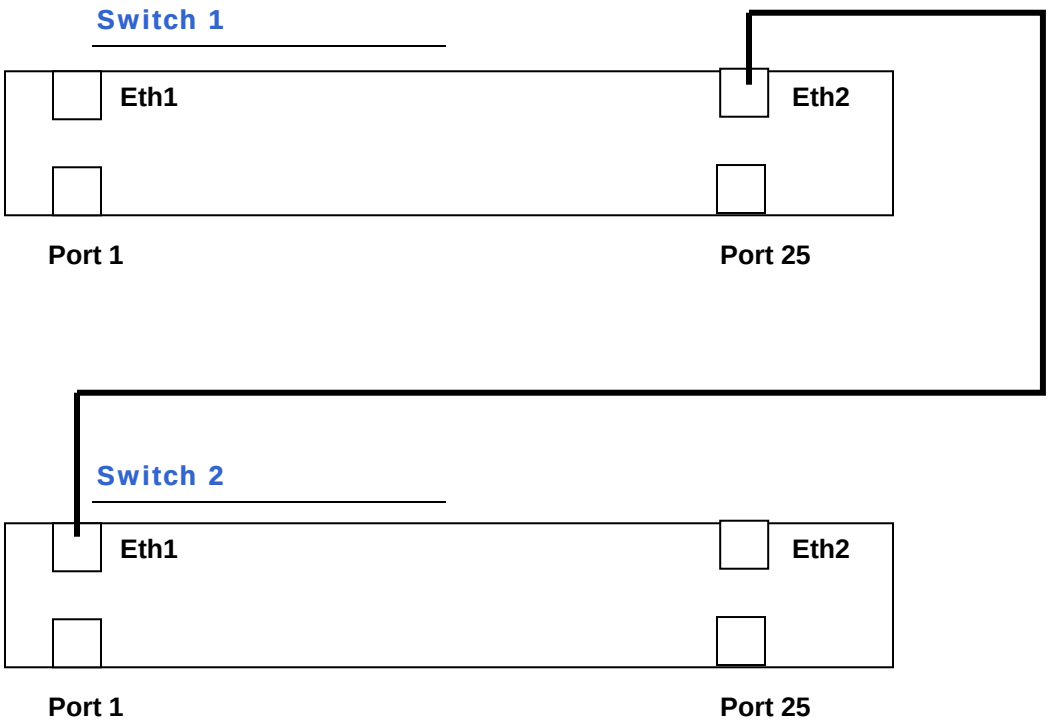
- WallPlate port 1 is used for HSIA. WallPlate port 2 is disabled to prevent the subscriber from using the wrong port.
- Eth1 is used for all packets. Eth2 is enabled as a cascade port.

Privacy and QoS in this network:

- Privacy enforced between all DSL ports using Port-based VLANs
- Privacy enforced between Eth2 and all DSL ports. Eth2 can only communicate with Eth1
- QoS is not used since there is a single service delivered to each user

VLAN-Ids used in this configuration:

- Port-based on Switch



Verify that all devices can ping each other before proceeding

Login to T2 via telnet or hyper-terminal,
From CLI type the following commands:

Enable VLANs, configure VLAN modes

```
vlan enable
vlan mode local-mode port-based remote-mode disabled
system reboot
```

Remove DSL ports from the Eth2 port-based VLAN

```
vlan port-group delete eth2 peer-interface port(1-25)
```

Optional configuration on the cascaded switch

Configure cascaded switch exactly as the first switch. Connect Eth1 of the cascaded switch to Eth2 of the first switch. Repeat for each cascaded switch.

Convert this tutorial to a real-world configuration

Note that in this tutorial, all packets are untagged ***outside*** of the T2. This allows for a very quick, simple installation of multiple switches since every switch can have the exact same configuration.

Be sure to NOT add all DSL ports to Eth2. This ensures that cascaded packets can only egress on Eth1

Create a configuration script following the command syntax for each step of the tutorial

Line Status

Operators can view extensive details about DSL line characteristics from the CLI, Port Monitor web page, or SNMP.

To view line characteristics using the webUI, click on DSL Monitor, then click the + sign to expand the port you wish to view.

Using the Port Monitor web page, the operator can quickly scan the status of all ports in the system. A color coded grid indicates the important status of each port e.g. GREEN indicates the Ethernet port is connected, whereas GREY indicates the port is enabled, but disconnected.

Per line details visible:

Status	Options are self-explanatory: disabled, enabled, linking, link lost, linked.
Quality	Link quality is a measurement of bit errors per second. Options are: Good, Fair, Bad. mT2 includes Forward Error Correction in the VDSL frames. Bit errors that are not corrected are counted and reported as a Line Quality measurement. Bit errors of 0 – 0.51 per second = Good Bit errors of 0.51 - 1 per second = Fair Bit errors of greater than 1 per second = Bad
Portx	Where “x” is the number of a remote Ethernet port on the WallPlate. Shows the status of the remote Ethernet port. Options are: connected, disconnected, disabled.
Downstream	Displays the line bitrate in the downstream direction in Mbits/second.
Upstream	Displays the line bitrate in the upstream direction in Mbits/second.
SNR DSx **SNR USx**	Where “x” is 1 or 2. mT2 uses a 4-band QAM modulation. Three of the 4 bands are used by mT2 to maximize downstream line bitrate. DS1 and DS2 refer to the two downstream bands; whereas US1 refers to the single upstream band. If a band shows 0 SNR, the band is not being used by that line. During normal operation, it will be common to see 0 SNR on DS2. US2 will always show 0, this is normal. SNR can be used to diagnose line issues, but must be considered in concert with other parameters. Values are in dB.
Margin DSx **Margin USx**	Each band requires SNR to be reserved as for margin. Typical values of SNR margin is between 6 and 9. If margin is lower than 6, the line may have low quality and may retrain at any time. If margin is greater than 9, the line is capable of a higher bitrate. Any band that is not being used will show a margin of 0. Values are in dB.
Distance (m)	Distance value shows estimated line length in meters, based on the level of the attenuated signal. Distance is accurate within 10% over 150m. Measurements below 150m are displayed at <150.

Line Current

This value indicated the total power consumed by the port; including power loss in the wire, in the WallPlate, and efficiency.

Maximum power for any single line: 9 watts
Maximum power for a complete system: 200 watts

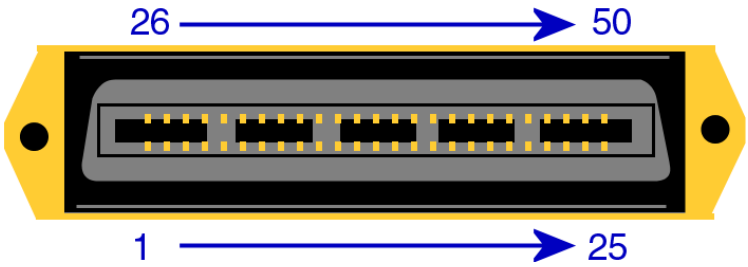
To determine the power for a single line use the following chart:

Line Current Value	Watts	Reference
255	2.58	Idle, no load or wire attached
197	4.87	
195	4.91	
190	5.02	
185	5.13	
180	5.31	
175	5.38	2m wire attached, no load
170	5.49	
165	5.60	
162	5.71	
160	5.82	
155	5.93	
150	6.11	
145	6.25	
140	6.40	
135	6.58	
130	6.80	
125	7.02	
120	7.24	
115	7.45	
113	7.53	
112	7.64	
110	7.71	
105	7.93	
100	8.18	
95	8.47	
90	8.76	
85	9.13	600m wire attached, 2 x 100Mb load
80	9.45	
75	9.85	
70	10.29	
65	10.76	
60	11.27	
55	11.78	
50	12.36	*Out of spec*
45	13.05	
40	13.64	
35	14.40	
30	15.53	
25	16.33	
20	17.49	

Appendix A: Pin-out Assignments

The rear of the switch has two RJ21 connectors; one for the LINE (also called PBX, PSTN, or System) connections and one for PHONE (also called House or Station) connections. The connector is wired as a 50 pin telco connector, as follows:

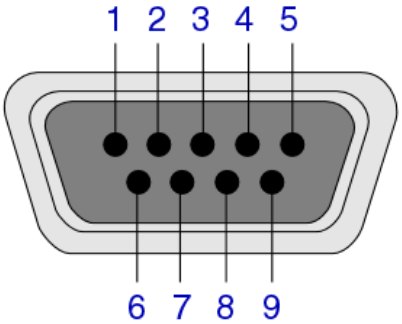
RJ21 Line Connectors



Pin 26 = line 1 Tip
Pin 1 = line 1 Ring
Pin 27 = line 2 Tip
Pin 2 = line 2 Ring

Pin 50 = line 25 Tip
Pin 25 = line 25 Ring

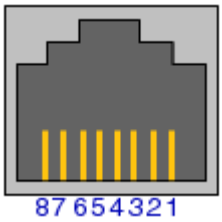
RS-232 console port



Pin 1	Unused
Pin 2	TXD – transmit data
Pin 3	RXD – receive data
Pin 4	Unused
Pin 5	GND – signal ground

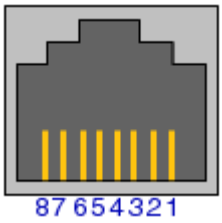
Pin 6	Unused
Pin 7	Unused
Pin 8	Unused
Pin 9	Unused

Gigabit Ethernet ports



1	BI_DA+	Bi-directional pair + A
2	BI_DA-	Bi-directional pair – A
3	BI_DB+	Bi-directional pair + B
4	BI_DC+	Bi-directional pair + C
5	BI_DC-	Bi-directional pair - C
6	BI_DB-	Bi-directional pair – B
7	BI_DD+	Bi-directional pair + D
8	BI_DD+	Bi-directional pair – D

Fast Ethernet WallPlate ports



1	TX+
2	TX-
3	RX+
4	Unused
5	Unused
6	RX-
7	Unused
8	Unused

Appendix B: Hardware Specifications

mT2 Switch

Line code modulation	3-band, QAM modulation Automatic power backoff, independent line-rate adaptation
Interfaces	2 x RJ45, 10/100/1000Mbps auto-sensing – 328ft (100m) 2 x RJ21, female telco connector 1 x dB9, female console port
Operating Voltage	100 – 240VAC, 50/60Hz
Power Consumption	300 Watts
Dimensions	17.25” x 14.25” x 1.75” (43.8cm x 36.1cm x 4.4cm)
Weight	11.5lbs (5.2Kg)
Environmental	Operating Temperature: 0 – 50 degrees Celsius, fan cooled
Relative Humidity	5% to 90% NC
Compliance	FCC Part 15A, CE, TUV EN60950
Telephone splitter	Integrated analogue POTS splitter
Management	In Band Management Telnet, Web UI, SNMP v2 standard and enterprise MIB Out of Band Management Console
Front Panel LEDs	1 x unit power status 25 x line link status 10/100/1000 link status, activity
Mounting Options	Rack mount ears provided

m2 WallPlate

Interfaces	2 or 4 x RJ45, 10/100/Mbps auto-sensing – 328ft (100m) 1 x RJ11, line-in port 1 x RJ11, filtered phone port
Operating Voltage	Local power supply (not provided): 12VDC, regulated supply
Power Consumption	2 watts
Dimensions	4.75” x 3.5” x 1.25” (120mm x 88mm x 32mm
Weight	0.5lbs (0.2Kg)
Environmental	Operating Temperature: 0 – 50 degrees Celsius
Relative Humidity	5% to 90% NC

Compliance	FCC Part 15A CE, TUV EN60950
Telephone splitter	Integrated analogue POTS splitter
Management	In Band Management Telnet, Web UI, SNMP v2 standard and enterprise MIB
Front Panel LEDs	1 x unit power/link status 10/100 link status, activity
Mounting Options	Mounting bracket provided

Appendix C: Compliance

FCC Part 15A

This device complies with part 15 of the FCC Rules. Operation is subject to two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT SAFETY INSTRUCTIONS
mT2a Switch
CAUTION: For installation only in a Restricted Access Location by trained service personnel.
CAUTION: Equipment must be connected to an earthed mains socket-outlet.
CAUTION – To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
CAUTION: The power supply cord plug serves as the main disconnect for the product. The socket-outlet shall be installed near the product and be readily accessible.
CAUTION: Voltages present which are above TNV-3 (POTS) limits. A cover must be installed over the punch down blocks with a HV (High Voltage) warning label (supplied).

The maximum operating ambient temperature is 50 degrees Celsius.

When installing the mT2a Switch in an equipment rack, consider the following potential hazards:

Elevated Operating Ambient Temperature – If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra).

Reduced Air Flow – Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading – Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit Overloading – Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing – Reliable earthing of rack-mounted equipment should be maintained.
Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

m2a WallPlate
CAUTION: Use only power supplies listed in the user manual

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.

2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

3. Do not use the telephone to report a gas leak in the vicinity of the leak.
SAVE THESE INSTRUCTIONS